

**REVOCATION AND UPDATING OF TOKENS IN
A PUBLIC KEY INFRASTRUCTURE SYSTEM**

ABSTRACT OF THE DISCLOSURE

A method and computer program to revoke and update a token (130) having several encryption, signature and role certificates/private keys contained in the token (130). The certificates/private keys in the token 130 are transmitted wrapped by a public key and may only be activated by a private key contained in the token (130). The activation of any certificate/private key requires the entry of a passphrase by a user (132). Further, all certificates/private keys contained in a token (130) are stored in an authoritative database 104. In the event that a token (130) is lost then all certificates/private keys associated with the token (130) are revoked. Further, when new certificates/private keys are issued to a user (132) these certificates/private keys are encrypted using the token's (130) public key and downloaded to the token (130).